

RISK MANAGEMENT

RedSeal Security Risk Manager

REVIEWED BY ADAM HOSTETLER

RedSeal Systems

www.redseal.net

Price: RedSeal SRM v2.0 is now available. End user pricing for a product license starts at \$10,000 and monthly subscriptions start at \$1,000 per month. Prices are subject to change. Downloads available at www.redseal.net.

Your network produces a flood of information that could tell you where your business is at greatest risk. But how do you sort through it all and determine exactly how your critical assets are threatened?

RedSeal's Security Risk Manager (SRM) enables security administrators to model and manage threats to those corporate assets and network infrastructure. The appliance transforms network device configurations, vulnerability data and system value ratings into a graphical view that shows how systems can be compromised.

Setup and Configuration **B**

Setup is fairly easy. We hooked up the serial cable, ran a few configuration commands and installed the SRM Java administrative application through our browser (only Windows is supported).

SRM generates risk and threat maps based on imported device configurations and vulnerability data. SRM supports popular network devices out of the box, including Cisco IOS, Cisco PIX5/6/7, Juniper ScreenOS and Check Point Firewall-1/VPN-1 NGX, as well as vulnerability sources such as Nessus and QualysGuard. Other devices can be imported with the help of RedSeal, or by creating an XML schema. Device and vulnerability data can be imported

Testing methodology: We tested the RedSeal SRM appliance using RedSeal-provided data that modeled a network containing a mixture of network devices, and vulnerability data, in addition to data generated in our lab.

manually, or SRM can retrieve it directly from the devices or a central repository through a variety of means (FTP, SSH, HTTP/S, Telnet, CVS).

Effectiveness **A**

SRM's clean tabbed interface nicely displays available information and makes it easy to import data or edit device and system values. This clean interface carries over into the network map, which appears quite haphazard at first, with systems appearing out of order and all over the map. This is quickly alleviated by the auto-arrangers, which are a great feature for larger networks. The map shows connectivity between devices and networks, accounting for traffic flow restricted and allowed by ACLs.

You can assign values (from 1-100) to systems to help determine where your company is at greatest risk. SRM uses this data to generate risk and threat maps.

The threat map is similar to the inventory map, but includes threat calculations based on exposure and business value, modeling how an attacker might get to a system, and through which vulnerabilities. You can pick any point in your network to see which systems can talk to this system, or what systems your selected system can see. A "heat box" style risk map shows which systems are at greatest risks and establishes mitigation priorities.

The threat map showed us systems at risk, such as firewalls allowing improper traffic, or systems that had severe vulnerabilities. After correcting the issues and reloading the data, we could regenerate the maps and see that the issues were mitigated. For instance, SRM showed that a high-value internal database server could be attacked from an FTP vulnerability on an external server. After the issue with the FTP server was mitigated, SRM showed that the database server was no longer threatened.

Reporting **B**

Reports can be generated for a number of different categories, including inventory, network device configuration errors, exposure to vulnerabilities and performance data of the appliance. The network configuration checks are quite useful, as they compare your network devices against a built-in rule set to check for common configuration errors. Some reports contain colorful heat bars, or expanding bubbles to show threats, others just text.

Verdict

RedSeal SRM is a very good tool to provide an overall view of network threats and risks, and will help you prioritize mitigation measures. •

Reprinted with permission from Information Security Magazine, June 2007.

© 2007 TechTarget. All Rights Reserved. FosteReprints: 1-866-879-9144



888-845-8169

info@redseal.net • www.redseal.net